RECEIVED
CENTRAL FAX CENTER

AUG 2 3 2006

Remarks

Claims 1-7 are pending in this application. Claims 1-7 stand finally rejected by Berg et al. (U.S. Patent Publication No. 2002/0188481; hereafter "Berg") under 35 U.S.C. § 102(e).

Before addressing the present rejections, a brief summary of the prosecution history is provided. In the office actions mailed 02/07/2005 and 07/15/2005, claims 1-5 were rejected under 102(e) over Harif (US 2002/0087881) which disclosed *inter alia* use of digital signatures. Applicants' responded in part by explaining that digital identity of the present invention is different from digital signatures and digital certificates because it does not involve installing/downloading software/program instructions (see page 5 of remarks filed 08/30/2005). Subsequently, in the non-final office action mailed 09/30/05, the arguments were deemed persuasive and the rejection under Harif was accordingly withdrawn. However at the same time, a new 102(e) rejection was made in view of newly discovered art to Brachtl (US 4,747,050) which required *inter alia* personal identity cards. Applicants' responded on 11/28/2005 with an amendment and remarks stating in part that according to the present invention, the User does not require a personal identity card in order to use digital identity. Subsequently, in the office action mailed 02/17/2006, the arguments were deemed persuasive and the rejection under Brachtl was accordingly withdrawn. However at the same time, new rejections under 102(e) and 103(a) were made in view of Teper et al. (US 5,815,665), which required *inter alia* users to download/install client software components, and Aziz (US 5,732,137). In the response dated 04/06/2006, applicants' amended the claims and provided remarks to explicitly explain that the User does not require received software (*e.g.*, in the form of proprietary software, digital certificates, etc.) to use digital identity (see, pages 4-5 of the remarks filed 04/06/2006; see also, page 5 of the remarks filed 08/30/2005). In the latest office action mailed 06/20/2006, the arguments were deemed persuasive and the rejections under Teper and Aziz were accordingly withdrawn. However, at the same time, a new final rejection 'as necessitated by applicants' amendment' was made under 102(e) in view of Berg et al. (US 2002/0188481) which uses *inter alia* digital certificates (which applicants' distinguished from previously). In view of the above summary and the following remarks, applicants' respectfully request reconsideration and withdraw of the final office action.

The prior art rejections are addressed below.

Rejections under 35 U.S.C. § 102(e)

In the Final Office Action mailed 06/20/2006, the Office rejected claims 1-7 under 35 USC § 102(e) as being anticipated by Berg. Applicant respectfully traverses this rejection and submits

that the disclosure of Berg does not anticipate the presently claimed invention for the following reasons.

Berg is generally directed toward providing insurance coverage for online transactions to reduce risks, such as fraud, associated with a web-based marketplace. Specifically, Berg generates and provides a financial product which can provide insurance coverage "guaranteeing" (*e.g.*, financially) the identity or financial viability of a user (or trading counterpart) and/or the completion of a transaction with a trading counterpart [0002]. The insurance coverage provides, in exchange for payment of a premium, assurance against *e.g., misidentification of a trading party* [0012], [0033]. Thus, rather than authenticating or positively identifying a User, Berg provides an online insurance product that compensates for the possibility of user misidentification, inability to pay for a transaction, etc.

The system of Berg discloses various "entities" including: users (20) (*e.g.*, marketplaces, buyers, sellers); a JV Authority (30); a Registration Authority (40); a Credential Issuing Authority (50); etc. (see, Figure 1). In operation, users (20) initially submit identifying information to a Joint Venture (JV) Authority (30). The JV Authority (30) processes the input information with information contained in a database of business information providers for verification [0007], [0063]. The JV authority (30) may itself be a business information provider (*e.g.*, Dun & Bradstreet) that provides business, financial, and/or quality assurance information. In addition, the business information provider may provide identity and financial information such as: contact information, financial risk assessment, financial viability, credit-worthiness, credit score, profitability, etc. [0005], [0006]. After verification is complete, the JV Authority (30) sends information regarding the user (20) to a Registration Authority (40) that can register the verified user (20) and request security credentials, such as a digital certificate, from a Credential Issuing Authority (50) [0007], [0017].

Regarding claim 1 and similarly rejected claim 5, the office action states on page 3: "where the JV authority corresponds to the recited central-entity." Applicants' respectfully disagree. Unlike the Central-Entity of the present invention, **the JV Authority does not perform authentication of a User based on digital identity**. Rather, the JV Authority (30) "verifies" identity and/or financial viability of trading counterparts or users by processing identifying user information in conjunction with business information obtained from business information providers. Such information corresponds to *e.g.*, contact information, profitability, etc. However, a user cannot be positively identified by the JV Authority as a result of comparing information inputted by the user with obtained/purchased business information. This is because such information can be easily obtained, intercepted, stolen or guessed by others, and therefore cannot provide positive proof as to the user's identity. Instead, the purpose behind the verification of Berg is to provide a *risk assessment* as to whether the user will be able to pay for a transaction. (It is also noted that nowhere does Berg mention authentication). Thus, Berg does

not teach where the JV Authority authenticates or positively identifies users - not to mention based on digital identity.

Berg also does not disclose **whereby the External-Entity may forward digital identity received from a User to the Central-Entity for authentication**. Contrary to the present invention, nowhere does Berg disclose or suggest that the seller is able to receive digital identity from the User. Instead, Berg discloses that both buyers and sellers submit their security credentials to an intermediate marketplace [0034]. However, such a marketplace introduces a large number of additional entities, intensifying the possibility of user information being intercepted, spoofed, and/or misappropriated. Advantageously, the present invention avoids this problem by enabling "digital identity" to be securely provided to the External-Entity without compromising the User's personal and/or confidential information.

Moreover, Berg fails to teach **wherein the User does not require use of software received from the Central-Entity to employ digital identity**. Berg discloses that a user receives security credentials, or unique identifiers (such as digital certificates) from the Registration Authority [0007]. However, digital certificates comprise files that are downloaded and/or installed on a user's computer. (It is also appreciated that "software" is conventionally understood to be a set of computer-executable instructions.) In paragraphs [0007] and [0011], Berg even states that the digital certificates may be "*downloaded and temporarily stored* on any computer being used by a user" to verify identity and *to facilitate subsequent interaction with trading counterparts* (emphasis added). Thus, users would be required to download/install software with the digital certificates of Berg. Conversely with the present invention, Users may employ digital identity without first being required to install/download software (*e.g.*, in the form of digital certificates, proprietary software, etc.) received from the Central-Entity.

It appears that the Office may not fully understand the nature of digital certificates by associating the digital certificates of Berg with "digital identity" of the present invention. Although applicants' distinguished between digital certificates and "digital identity" on page 5 of the remarks filed 08/30/2005, the Office continues to apply prior art that relies upon digital certificates. Therefore, in response to the Final Office Action, two publications (www.computing.vt.edu/security_and_viruses/certificates/index.html; and "United States Patent and Trademark Office Public Key Infrastructure Subscriber Agreement," version 30) are included in Appendix A at the end of this communication to illustrate that *digital certificates involve users receiving software from a Central-Entity to download/install on their computers* – contrary to the present invention as claimed.

As an alternative to digital certificates, Berg very briefly mentions that the unique identifier may also refer to user name, password or alphanumeric identifier [0037]. However, "digital identity" is not the same as a password, user name or alphanumeric identifier. The problem with user names and passwords, etc. is that they are highly susceptible to being stolen, intercepted, or

guessed, and are thus not conventionally considered to be reliable means in themselves for authenticating, or positively identifying, a user. Advantageously, "digital identity" provides more security than just a password, user name or alphanumeric identifier. For example, according to one embodiment, digital identity includes a SecureCode and other information such as UserName and is entirely non-predictable such that the User's personal information remains highly secure. Because of this, the External-Entity may receive digital identity from the User without their personal or confidential information being compromised. This is not so with the passwords or user names of Berg. Transmission of passwords or user names to the External-Entity (in place of digital identity) would render the present invention inoperable and/or pointless as the User's personal or confidential information would be exposed and security compromised.

Furthermore, the participants of Berg are limited to those registered in the marketplace. In situations where External-Entities (*e.g.*, government agencies, universities and financial institutions) do not participate in such a marketplace, the system of Berg does not offer any solution or added-value. Examples of identity authentication in relation to such entities include where: the customer applies for government services over the internet; applies to vote online; applies for mortgage online; applies for a new credit card online, etc. In these examples, the External-Entities do not sell negotiable products and therefore cannot participate in Berg's marketplace. Thus, Berg's marketplace would not provide any value to such entities.

In an offline world, businesses authenticate customers' identity by looking at the customer's driver's license or identity card. In the online world, however, businesses currently do not have a *simple or cost effective* alternative to securely authenticate a user's online identity. Systems such as those taught by Berg are usually too complicated to reach the mass market. One reason for this being that the process of downloading and installing digital certificates is too time-consuming and/or burdensome. For example, users may not be computer-literate enough to know how to download and install a digital certificate. Moreover, the transaction may comprise a small, one-time transaction that doesn't justify the amount of effort involved in obtaining a digital certificate. Alternate authentication efforts using smart cards have also failed to take off since these introduce their own set of prohibitive implementation costs and burdens. Thus, in contrast to digital certificates and smart cards, digital identity of the present invention fills the authentication gap that exists in the online world today by providing a secure and cost effective solution that is easier to implement and use. Moreover, because digital identity increases trust in transactions, businesses can experience reduced risk and increased revenue as a result.

To anticipate a claim, the reference must teach every element of the claim: "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See MPEP 2131.

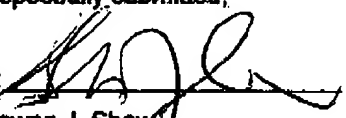
However, Berg fails to disclose each and every claimed limitation as evidenced in the above discussion regarding similarly rejected claims 1 and 5. Accordingly, Applicants' submit that claims 1 and 5 and their dependents are allowable over the prior art and request that the current rejection be withdrawn.

Conclusion

Applicants' respectfully request reconsideration of the claim rejections based on the above amendments and remarks. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 08/23/2006

By: 

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091

Appendix A - Document 1

[VirginiaTech]

Search: Go

computing.vt.edu

Digital Certificates at Virginia Tech

To promote the use of digital certificates, the e-Provisioning Group has established the Virginia Tech Certification Authority (VTCA) to provide a digital certificate service to the campus community. The VTCA is a service of Virginia Tech that is responsible for issuing and managing digital certificates and public keys for Virginia Tech affiliated entities. The VTCA guarantees the identity and the authenticity of the entities to which it issues digital certificates by using approved policies and procedures outlined in the Virginia Tech X.509 Certificate Policy (PDF, 152 KB) document.

Contents

Directory Tools

- People Search
- PID Information

Related Tasks

- ED Usage Requirements **(PDF, 15 KB)**
- Requesting ED-ID Service

Related Departments

- Information Resource Management (IRM)

Introduction

The VTCA is the core of the Virginia Tech Public Key Infrastructure (PKI) which is a set of comprehensive system policies, procedures, people, and technologies working together to allow secure and confidential communication between Internet users, including the ability to issue, maintain, and revoke digital certificates. To reinforce security measures, digital certificates are digitally signed by a third party known as a certification authority. PKI provides the critical element of trust in electronic transactions as well as communications. It provides a means for relying parties to know that another individual's or entity's public key actually belongs to that individual or entity.

Digital certificates provide secure connections to electronic services and can be issued to organizations and devices in addition to people. A Certification Authority is a trusted third party that verifies the identity of an entity registering for a digital certificate. Once a Certification Authority authenticates the requesting entity's identity, it issues a digital certificate to the requesting entity binding his or her identity to a public key. All digital certificates have an explicit start date and an explicit expiration date. Most applications check the validity period of a certificate when the digital certificate is used.

For more information about digital certificates, see the following:

- The Corporation for Research and Educational Networking (CREN)'s PKI Resources
- RSA Laboratories' Public-Key Cryptography Standards
- Internet2's Certificates and PKI

Virginia Tech Certification Authority Components

Digital certificates are electronic identity credentials which use encryption to support secure access to a large number of Web services and applications on campus. Initially, the VTCA is issuing server certificates which are digital credentials that reside on a server and set up a secure connection between that server and a client or another server. This secure connection uses PKI through either a Secure Sockets Layer (SSL) session or a Transport Layer Security (TLS) session. The relationship between PKI and security lies in the fact that the public and private keys can be used for encryption, or hiding the content of data as it is being transmitted over the network.

For Desktop Users

In order to realize the security benefits of digital certificates issued by the VTCA, all faculty, staff and students are encouraged to install the VTCA root certificate on their Web browsers. After installing the Virginia Tech root certificate, applications using certificates will automatically recognize and accept certificates issued by the VTCA.

If the root certificate is not installed in your Web browser, you may receive security warning messages or annoying pop-up windows asking if you trust the VTCA when accessing secure services that use VTCA issued certificates. Depending on your operating system and browser settings, you may see these warning messages every time you access secure servers which are using certificates issued by the VTCA. Downloading and installing the VTCA root certificate into your browser will help you prevent these recurring messages from appearing.

Eventually, the VTCA service will be expanded to issue Personal Digital Certificates to faculty, staff and students.

Root Certificate Download and Installation

You will need to complete the installation of the root certificate for each

browser you use on your computer and for each different computer. For example, you may use one computer at work and another one at home. Also, if you are using an older version of your browser, please upgrade your browser before installing the certificate.

To install the root certificate, choose one of the following sets of instructions according to the browser you use:

- Firefox
- Internet Explorer 6 in Windows
- Mozilla 1.7
- Netscape 8 in Windows
- Netscape 7 in Windows and Mac OS X
- Safari in Mac OS X v10.3/10.4
- Safari in Mac OS X v10.2

Personal Digital Certificates

In the future, Personal Digital Certificates will be offered to students, faculty, and staff for digitally signing documents. Personal certificates will be installed onto smart cards or tokens and can be used for authenticating to Web applications as well as sending or receiving secure e-mail. The VTCA will play an increasingly significant role by providing several important security functions including strong digital identity credentials for authentication; strong encryption for data communications and storage privacy; digital signatures which support non-repudiation of online transactions; and document integrity using digital signatures.

For Server Administrators

Middleware Certificate

The Virginia Tech Middleware Application Certification Authority (CA) enables SSL authentication and encryption for application servers connecting to the Virginia Tech ED (Enterprise Directory) authentication and authorization services using SSL, or TLS protocols.

- **To review the formal policy,** refer to the Virginia Tech X.509 Certificate Policy **(PDF, 152 KB)** document.
- **To obtain a Middleware Client Certificate,** refer to Requesting a Virginia Tech Middleware Certificate Authority.
- **To use OpenSSL,** refer to Using OpenSSL to Make a Request for a Virginia Tech Certification Authority (VTCA) Server or Application Certificate.

Middleware Certificate Profiles:

- Virginia Tech Middleware CA Certificate Profile **(PDF, 89 KB)**
- Virginia Tech Middleware Client Certificate Profile **(PDF, 35 KB)**
- Virginia Tech Middleware Server Certificate Profile **(PDF, 36 KB))**
- Virginia Tech Middleware Test Client Certificate Profile **(PDF, 35 KB)**
- Virginia Tech Middleware Test Server Certificate Profile **(PDF, 36 KB)**

For more information on ED, refer to the Enterprise Directory page.

Server Certificate

The Virginia Tech Class 1 Server Certification Authority enables SSL authentication and encryption services for networked application servers such as Web servers or e-mail. Application servers connecting to Virginia Tech computing resources with authentication and authorization services must use a digital certificate in order to communicate over a secured communication channel using SSL or TLS protocols.

- **To review the formal policy,** refer to the Virginia Tech X.509 Certificate Policy **(PDF, 152 KB)** document.
- **To obtain an SSL Server CA,** refer to Requesting a Virginia Tech Class 1 Server Certificate Authority.
- **To use OpenSSL,** refer to Using OpenSSL to Make a Request for a Virginia Tech Certification Authority (VTCA) Server or Application Certificate.

Server Certificate Profiles:

- Virginia Tech Class 1 Server CA Profile **(PDF, 90 KB)**
- Virginia Tech Class 1 Application Server Profile **(PDF, 129 KB)**
- Virginia Tech Class 1 Web Server Profile **(PDF, 129 KB)**

General Documentation

- **Frequently Asked Questions**
- **Glossary of Terms**
- **Policies**
  - Virginia Tech PKI Policy Management Authority **(PDF, 22 KB)**
  - Virginia Tech X.509 Certificate Policy Document **(PDF, 152 KB)**
  - Certification Practices Statement
- **Presentations**
  - Client SSL Authentication **(PPT, 74 KB)**
  - DCSS Fall 2004 Presentation - VTCA Service **(PPT, 398 KB)**
  - DCSS Fall 2003 Presentation - Introduction to the VTCA **(PPT, 215 KB)**
  - Security Task Force Presentation - Strong Authentication Technologies **(PPT, 7121 KB)**

Obtaining Further Assistance

If you need help installing VTCA certificates or have other questions, please contact 4help by using the Help Request Form or by calling (540) 231-HELP (4357).

Last updated on August 19, 2005

Appendix A - Documents

United States Patent and Trademark Office
Public Key Infrastructure
Subscriber Agreement

I request that the United States Patent and Trademark Office (USPTO) issue me a set of public key certificates (a digital signing certificate and a confidentiality certificate)[1] in accordance with conditions stated herein. I have read and signed the Certificate Action Form [PTO Form-2042] requesting issuance of public key certificates to me for doing business with the USPTO.

I agree that my use and reliance on the USPTO public key certificates is subject to the terms and conditions set out below. By signing the Certificate Action Form [PTO Form-2042] I agree to the terms of this Subscriber Agreement and to the rules and policies of the USPTO.

1. **Identification Information**

   a) I warrant that the information I submit, as corrected or updated by me periodically, is true and complete.

   b) If any of the information contained in the Certificate Action Form [PTO Form-2042] changes, I agree to update my information within 10 working days via written communication sent to Mail Stop EBC, Commissioner for Patents PO Box 1450, Alexandria, VA 22313-1450. This includes loss of right to access a given customer number.

2. **Protection of Keys**[1].

The USPTO will not have a copy of my private key corresponding to the public key contained in the digital signing certificate. I understand that the password I establish in the client software is my responsibility and that the password is unknown to the USPTO. Further, there is no mechanism for the USPTO to find the password. In the event of a lost password, as in the event of the loss of my private key(s), the USPTO can, at my request, recover only the private key corresponding to the public key contained in the confidentiality certificate and authorize the generation of a new digital signing public/private key pair.

   a) I agree to keep all password and private key(s) confidential, and to take all reasonable measures to prevent the loss, unauthorized disclosure, modification or use of any password(s), and private key(s). I agree that I will be responsible for these items and that no unauthorized person will have access to them.

   b) I agree and acknowledge that, when the USPTO issues me the information permitting me to generate a certificate, the USPTO will keep a copy of my private key corresponding to the public key of my confidentiality certificate, and the USPTO will not disclose this key except with my consent, or where required by law

---

[1] Each public key certificate includes the public key of a public/private key pair. The digital signing key pair is generated by the subscriber's personal computer via software provided by the USPTO and the public key becomes part of the digital signing certificate. Only the subscriber holds the private key corresponding to the public key contained in the digital signing certificate. Both the public and private keys of the confidentiality certificate will be generated by the USPTO Certificate Authority and sent via a secure channel to the subscriber. The USPTO Certificate Authority will hold a copy of the subscriber's private key corresponding to the public key contained in the confidentiality certificate in order to provide key recovery capability.

c) I agree to promptly notify the USPTO if my password(s) or private key(s) are lost, compromised or rendered insecure, or if the information contained in my certificate request, including address, e-mail address, or telephone number, has changed, or becomes otherwise incorrect or incomplete.

3. Acceptable Use or Reliance/Designation of Supervised Employee

I will use my USPTO certificates only for electronic communication with the USPTO (e.g., Patent Application Information Retrieval (PAIR) status inquiry, electronic filing, etc.). I will use or rely on USPTO certificates only for securing communication with the USPTO, and will not encourage or permit anyone other than the USPTO to rely on them.

I may designate an employee who may use my USPTO certificates at my direction. The designated employee may, acting at my direction and under my control file, a patent application or follow-on papers. The employee will use or rely on granted USPTO certificates only for communication with the USPTO and will not encourage or permit anyone other than the USPTO to rely on them. I understand that I am responsible for the employee's use of the USPTO certificates. I agree not to use or permit the use of my USPTO certificate in connection with the unauthorized practice of law. If I have been granted limited recognition by the Office, I agree not to use the digital certificate beyond the limits of the rights I have been granted.

I understand that my USPTO certificate will be used to access records and systems on a U.S. Government computer system and that unauthorized use or use beyond the purpose authorized may subject me to criminal penalties under U.S. Law.

4. Revocation of Certificates

a) The USPTO may revoke my certificate(s) at any time without prior notice if:
i. any of the information I supply in my certificate(s) request changes;
ii. the USPTO knows or suspects that my private key(s) has/have been compromised
iii. the private key(s) of the issuing USPTO Certificate Authority has/have been compromised;
iv. the signing certificate of the issuing USPTO Certificate Authority is revoked;
v. I fail to comply with my obligations under this Agreement; or
vi. for any other reason the USPTO deems necessary.

The USPTO will promptly notify me of the revocation. Such revocation does not affect the authenticity of a transmission made or a message I digitally signed before certificate revocation.

b) I may surrender my certificate(s) at anytime by written submission to the USPTO at:

Certificate Services Request
U.S. Patent and Trademark Office
Mail Stop EBC
PO Box 1450
Alexandria, VA 22313-1450

5. Software use

I agree to honor any applicable copyright, patent, or license agreements with respect to any software provided to me by the USPTO, and will not tamper with, alter, destroy, modify, reverse engineer, or decompile such software in any way. I agree not to use the software for any purpose other than communication with the USPTO.

6. Restrictions on the Export of Patent Applications: Deemed Export in the U.S.

I understand that technology included in patent applications may be subject to export control regulations, and I agree not to use or permit the use of the USPTO certificate in a manner that would violate or circumvent these regulations

7. Software Export Restrictions

Cryptographic Software Notice and Acknowledgement

Notice:
The USPTO Direct software includes cryptographic software subject to export controls under the Export Administration Regulations and anyone receiving the software by download or otherwise may not export the software without a license.

Acknowledgement:

I understand that the cryptographic software I receive or download is subject to export controls under the Export Administration Regulations and that I may not export the software without a license.

References to the Export Administration Regulations are references to 15 CFR chapter VII, subchapter C. They are issued by the United States Department of Commerce, Bureau of Industry and Security (BIS) under laws relating to the control of certain exports, reexports, and activities.

By downloading, installing or using the USPTO supplied Software I am representing and warranting that I am not located in, under the control of, or a national or resident of any country to which the export of the Software or related information would be prohibited by the laws of the United States. At this time these countries include Cuba, Iran, Libya, North Korea, and Syria. This list reflecting the information in the Export Administration Regulations Supplement No. 1 to Part 740S page 7 and the other export control notifications administered by the Department of the Treasury will be periodically updated on the EBC website.

8. Availability

I understand that the USPTO does not warrant or represent 100% availability of the USPTO Public Key Infrastructure services due to system maintenance, repair, or events outside the control of the USPTO. Information regarding scheduled downtime, if known, will appear on the USPTO Electronic Business Center web site. Any delays caused by downtime must be addressed through the ordinary petition process.

9. Term of Agreement

This Agreement may be terminated by either party upon proper notice. In the case of a termination by the USPTO, notice may provided any reasonable means, including a posting on the USPTO website.

10. General

If any provision of this Agreement is declared by a court to be invalid, illegal, or unenforceable, all other provisions shall remain in full force and effect.

The USPTO reserves the right to refuse to issue certificates. The USPTO reserves the right to cancel this program at any time. Modifications to this agreement will be posted on the USPTO website at www.uspto.gov/ebc/efs. Continued use of the system after posting will constitute agreement to the updated terms.

11. Requests

Requests for issuance of certificates, revocation of certificates or key recovery shall be sent to the USPTO Registration Authority at:

Certificate Services Request
U.S. Patent and Trademark Office
Mail Stop EBC
PO Box 1450
Alexandria, VA 22313-1450

12. Dispute Resolution and Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the United States of America.